

PATENT ABSTRACTS OF JAPAN

(11) Publication number : 2002-073565
 (43) Date of publication of application : 12. 03. 2002

(51) Int. Cl. G06F 15/00
 H04L 9/32

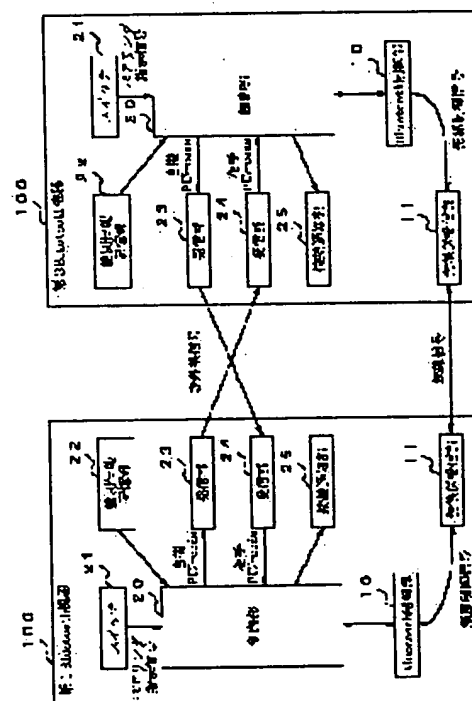
(21) Application number : 2000-266401 (71) Applicant : NEC CORP
 (22) Date of filing : 04. 09. 2000 (72) Inventor : MIURA TAKAO

(54) SYSTEM AND METHOD FOR AUTHENTICATING ELECTRONIC EQUIPMENT

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a system and a method for authenticating electronic equipment by which authentication is performed by mutually exchanging identification information by a simple operation.

SOLUTION: The authentication system for electronic equipment is provided with a switch 21 for permitting a user to instruct to perform authentication, an identification information storage part 22 for recording data on identification information of its own machine, an emitting part 23 for emitting identification information to the electronic equipment of an opposite side to connect by using an infrared signal, a reception part 24 for receiving data on the identification information of the electronic equipment of the opposite side to connect which is emitted from the electronic equipment of the opposite side to connect by using the infrared signal, a connection informing part 25 for informing the user that the mutual exchange of data on identification information is successfully completed by the lighting of a light emitting diode and a locking mechanism 26 for locking the performance of an authentication processing by interlocking a switch 21 with a cylinder lock with key. Data on identification information is mutually exchanged with the electronic equipment of the opposite side to connect in accordance with the instruction for performing authentication by the switch 21. Then, the authentication processing is performed on the basis of received data of identification information of the electronic equipment of the opposite side to connect.



LEGAL STATUS

[Date of request for examination]

21. 08. 2001

BEST AVAILABLE COPY

[Date of sending the examiner's decision
of rejection]

[Kind of final disposal of application
other than the examiner's decision of
rejection or application converted
registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against
examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998, 2003 Japan Patent Office

(51) Int.Cl. ⁷	識別記号	F I	ターム(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 C 5 B 0 8 5
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 B 5 J 1 0 4

審査請求 有 請求項の数22 O L (全 10 頁)

(21) 出願番号 特願2000-266401(P2000-266401)

(22) 出願日 平成12年9月4日(2000.9.4)

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 三浦 高生

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100093595

弁理士 松本 正夫

Fターム(参考) 5B085 AED4

5J104 AA07 KA02 KA07 NA01 NA36

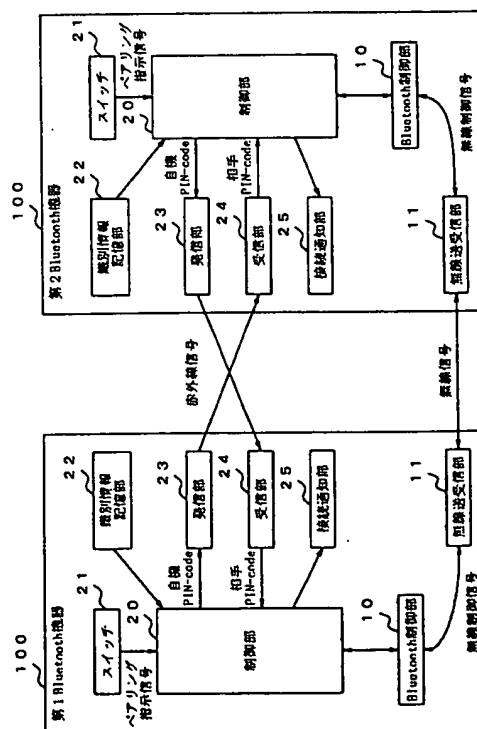
NA38 NA43

(54) 【発明の名称】 電子機器の認証システムとその認証方法

(57) 【要約】

【課題】 簡単な操作により識別情報を相互に交換して認証を行うことのできる、電子機器の認証システムとその認証方法を提供する。

【解決手段】 電子機器の認証システムにおいて、利用者が認証の実行を指示するためのスイッチ21と、自機の識別情報のデータを記録する識別情報記憶部22と、識別情報を接続相手の電子機器に対し赤外線信号を用いて発信する発信部23と、接続相手の電子機器から赤外線信号を用いて発信される接続相手の電子機器の識別情報のデータを受信する受信部24と、発光ダイオードの点灯により識別情報のデータの相互の交換が無事完了したことを利用者に通知する接続通知部25と、スイッチ21を鍵付きのシリンダー錠に連動させることにより認証処理の実行に対しロックを掛けるロック機構26を備え、スイッチ21による認証の実行の指示に応じて、接続相手の電子機器との間で識別情報のデータを相互に交換し、受信した接続相手の電子機器の識別情報のデータに基づき認証処理を実行することを特徴とする。



【特許請求の範囲】

【請求項 1】 電子機器の認証システムにおいて、
 自機を識別する識別情報のデータを記録する識別情報記憶部と、
 前記識別情報を接続相手の電子機器に対し発信する発信部と、
 前記接続相手の電子機器から発信される、前記接続相手の電子機器の識別情報のデータを受信する受信部を備え、
 利用者による認証を指示する操作に応じて、前記接続相手の電子機器との間で識別情報のデータを相互に交換し、受信した前記接続相手の電子機器の識別情報のデータに基づき認証処理を実行することを特徴とする電子機器の認証システム。

【請求項 2】 前記識別情報を、ブルートゥース機器の PIN-code とすることを特徴とする請求項 1 に記載の電子機器の認証システム。

【請求項 3】 前記発信部及び前記受信部は、
 赤外線信号を用いて、前記識別情報のデータを送受することを特徴とする請求項 1 又は請求項 2 に記載の電子機器の認証システム。

【請求項 4】 前記接続相手の電子機器との間における、識別情報のデータの相互の交換が無事に完了した場合にその旨を利用者に通知するための接続通知部を備えることを特徴とする請求項 1 から請求項 3 のいずれか一つに記載の電子機器の認証システム。

【請求項 5】 前記接続通知部は、
 発光ダイオードの点灯により、識別情報のデータの相互の交換が無事に完了したことを利用者に通知することを特徴とする請求項 4 に記載の電子機器の認証システム。

【請求項 6】 認証処理の実行に対しロックを掛けるロック機構を備え、
 前記ロック機構においてロックが掛けられている場合には、認証を実行しないことを特徴とする請求項 1 から請求項 5 のいずれか一つに記載の電子機器の認証システム。

【請求項 7】 自機を識別する識別情報のデータを記録する識別情報記憶部と、
 前記識別情報を接続相手の電子機器に対し発信する発信部と、
 前記接続相手の電子機器から発信される、前記接続相手の電子機器の識別情報のデータを受信する受信部を備え、
 利用者による認証を指示する操作に応じて、前記接続相手の電子機器との間で識別情報のデータを相互に交換し、受信した前記接続相手の電子機器の識別情報のデータに基づき認証処理を実行することを特徴とする電子機器。

【請求項 8】 前記発信部及び前記受信部は、
 赤外線信号を用いて、前記識別情報のデータを送受する

ことを特徴とする請求項 7 に記載の電子機器。

【請求項 9】 前記接続相手の電子機器との間における、識別情報のデータの相互の交換が無事に完了した場合にその旨を利用者に通知するための接続通知部を備えることを特徴とする請求項 7 又は請求項 8 に記載の電子機器。

【請求項 10】 前記接続通知部は、
 発光ダイオードの点灯により、識別情報のデータの相互の交換が無事に完了したことを利用者に通知することを特徴とする請求項 9 に記載の電子機器。

【請求項 11】 利用者が認証の実行を指示するためのスイッチと、
 自機を識別する識別情報のデータを記録する識別情報記憶部と、
 前記識別情報を接続相手の電子機器に対し赤外線信号を用いて発信する発信部と、
 前記接続相手の電子機器から赤外線信号を用いて発信される、前記接続相手の電子機器の識別情報のデータを受信する受信部と、
 発光ダイオードの点灯により、識別情報のデータの相互の交換が無事に完了したことを利用者に通知する接続通知部を備え、
 前記スイッチによる認証の実行の指示に応じて、前記接続相手の電子機器との間で識別情報のデータを相互に交換し、受信した前記接続相手の電子機器の識別情報のデータに基づき認証処理を実行することを特徴とする電子機器。

【請求項 12】 前記識別情報を、ブルートゥース機器の PIN-code とすることを特徴とする請求項 7 から請求項 11 のいずれか一つに記載の電子機器。

【請求項 13】 認証処理の実行に対しロックを掛けるロック機構を備え、
 前記ロック機構においてロックが掛けられている場合には、認証を実行しないことを特徴とする請求項 7 から請求項 12 のいずれか一つに記載の電子機器。

【請求項 14】 前記ロック機構は、
 利用者が認証の実行を指示するためのスイッチを、鍵付きのシリンダー錠に連動させるものとすることを特徴とする請求項 13 に記載の電子機器。

【請求項 15】 電子機器の認証方法において、
 利用者からの認証の実行の指示を受け付けるステップと、
 記録されている自機を識別する識別情報のデータを読み出し取得するステップと、
 前記自機の識別情報のデータを、接続相手の電子機器に対し発信するステップと、
 前記接続相手の電子機器から発信される、前記接続相手の電子機器の識別情報のデータを受信するステップを備え、
 利用者による認証を指示する操作に応じて、前記接続相

手の電子機器との間で識別情報のデータを相互に交換し、受信した前記接続相手の電子機器の識別情報のデータに基づき認証を実行することを特徴とする認証方法。

【請求項16】 前記識別情報を、ブルートゥース機器のPIN-codeとすることを特徴とする請求項15に記載の認証方法。

【請求項17】 赤外線信号を用いて、前記識別情報のデータを送受することを特徴とする請求項15又は請求項16に記載の記載の認証方法。

【請求項18】 前記接続相手の電子機器との間における、識別情報のデータの相互の交換が無事に完了した場合に、その旨を発光ダイオードの点灯により利用者に通知するステップを備えることを特徴とする請求項15から請求項17のいずれか一つに記載の認証方法。

【請求項19】 コンピュータシステムを制御することにより電子機器の認証処理を制御する、コンピュータプログラムを記録した記録媒体において、利用者からの認証の実行の指示を受け付けるステップと、

記録されている自機を識別する識別情報のデータを読み出し取得するステップと、

前記自機の識別情報のデータを、接続相手の電子機器に対し発信するステップと、

前記接続相手の電子機器から発信される、前記接続相手の電子機器の識別情報のデータを受信するステップを備え、

利用者による認証を指示する操作に応じて、前記接続相手の電子機器との間で識別情報のデータを相互に交換し、受信した前記接続相手の電子機器の識別情報のデータに基づき認証処理を実行することを特徴とするコンピュータプログラムを記録した記録媒体。

【請求項20】 前記識別情報を、ブルートゥース機器のPIN-codeとすることを特徴とする請求項19に記載のコンピュータプログラムを記録した記録媒体。

【請求項21】 赤外線信号を用いて、前記識別情報のデータを送受することを特徴とする請求項19又は請求項20に記載のコンピュータプログラムを記録した記録媒体。

【請求項22】 前記接続相手の電子機器との間における、識別情報のデータの相互の交換が無事に完了した場合に、その旨を発光ダイオードの点灯により利用者に通知するステップを備えることを特徴とする請求項19から請求項21のいずれか一つに記載のコンピュータプログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、電子機器相互間の認証処理に関し、特に各電子機器を識別する識別情報の交換を効率的に行う電子機器の認証システムとその認証方法に関する。

【0002】

【従来の技術】 電子機器においては、接続相手の機器の認証を行い、接続の許可された正しい接続先の機器に限りその接続を行うものがある。このように、接続相手の機器の認証を行うことにより、各電子機器に記録された情報の漏洩が防止され、不適切な接続による電子機器の破損等が防止される。また、特に無線通信により電子機器が通信する場合においては、認証によって、受信する電波の中から通信相手の電子機器からの無線電波を正しく識別することができ、又送受する信号が他の機器に漏洩しないように暗号化した信号を送受することもできる。こうした、無線通信による電子機器の通信には、例えば、無線通信規格Bluetooth（ブルートゥース、短距離無線システム）による通信がある。

【0003】 Bluetoothとは、ノートパソコンや携帯電話等の各種装置間を、廉価で高速に通信する小型の無線LANシステムの規格である。

【0004】 Bluetoothによる通信機能を備える機器（以下、これをBluetooth機器と呼ぶ）においては、近いエリア内におけるデータや音声の高速の全二重通信が可能であり、その通信には特殊な暗号化や認証を使用している。このため、Bluetooth機器においては、従来のようにケーブルを必要とすることなく、各種のパソコン等の情報機器や携帯電話等の通信機器を接続することができる。

【0005】 また、インターネット上のBluetoothの公式サイトである“The Official Bluetooth SIG Website”（<http://www.bluetooth.com/>）においては、Bluetoothの仕様を一般に公開しており、このサイトからBluetoothの仕様が記載されたPDFファイルをダウンロードすることができる。このBluetoothの仕様書は、Core編とProfile編の2部構成による、“Specification of the Bluetooth System v1.0 B, Wireless connections made easy, (Specification Volume 1 Core), (Specification Volume 2 Profiles), 1999年12月1日”であり、“<http://www.bluetooth.com/developer/specification/specification.asp>”から、この2本の仕様書をダウンロードすることができる。

【0006】 図5は、従来のBluetooth機器100cの構成を示すブロック図である。

【0007】 図5を参照すると、従来のBluetooth機器100cにおいては、Bluetoothによる通信を制御するBluetooth制御部10、Bluetoothにおける無線通信を行う無線送受信部11、認証処理を制御する制御部20、各機器を識別する識別情報であるPIN-codeの入力を行うための入力部12、入力したPIN-code等を表示する表示部13を備えている。

【0008】 PIN-codeとは、各Bluetooth機器を識別するための固有の番号であり、1～16オクテットの長さを持つビット列としてBluetoothの仕様に規定されるもの

である。

【0009】Bluetooth機器においては、接続相手の機器のPIN-codeを予め取得し、その接続する2端末間において共有するセキュリティ保持のためのパラメータであるLin-Keyを双方の機器において生成し保持する。これにより、以後の双方の機器間の通信においては、この共有するLin-Keyを元に認証を行い通信データを暗号化することにより、接続時や通信時においてその相手機器が正しい接続相手の機器であるかを確かめることができ、正常に通信を行うことができる。

【0010】しかし、このように認証処理を行う電子機器では、他の電子機器との間において認証された通信を行うためには、その接続相手の機器のPIN-code等の識別情報の入力が必要とし、接続相手の機器の識別情報をまだ取得していない状態においては、通信を行うことができない。

【0011】このため、例えばBluetooth機器を最初に接続する時においては、まず、その双方のBluetooth機器のそれぞれに対し接続相手の機器のPIN-codeを入力し、その最初の接続手続きを行う。このように、PIN-codeを相互に入力して最初のBluetooth接続手続きを行うことを、Bluetooth規格の用語でペアリング(Pairing)と呼ぶ。

【0012】Bluetoothでの無線接続をする場合に、買ってきたばかりのBluetooth機器同士等では、Link-keyの交換がなされていないために接続できない。このため、最初の手順としては、Link-keyの代わりにPIN-codeを相互に入力して最初の接続を開始する。PIN-codeを使って接続した際に、Link-keyの生成が行われ互いのデータベースに登録されることで、次回からはLink-keyによる接続が可能になる。

【0013】また、Bluetooth機器へのPIN-codeの入力は、図5に示されるようにテンキー等の入力部12から入力するのであり、液晶パネル等の表示部13にその入力したPIN-codeを表示させて参照しながらその入力を行う。

【0014】こうした、液晶パネルやテンキー等の入力部12や表示部13は、認証処理を管理する制御部20の制御下にあり、テンキーから入力された相手機器のPIN-code情報は、この制御部20を介してBluetooth制御部10に伝達される構成である。

【0015】相手機器のPIN-codeは、このように利用者が手操作により入力するのであり、図5の例においては、第1Bluetooth機器に対しては第2Bluetooth機器PIN-codeを入力し、かつ第2Bluetooth機器に対しては第1Bluetooth機器PIN-codeを入力するのである。

【0016】Bluetooth制御部10には、例えば、MITEL社 (<http://www.mitel.com>) のMT1020Aチップ等が用いられている。MT1020Aチップにおいては、制御部20からの相手PIN-codeの通知を、そのMT1020AチップのHOST

UARTインタフェースを介して伝達を受けている。

【0017】制御部20においては、例えば、Bluetooth機器のペアリングを処理するためのコンピュータプログラムを搭載したマイクロプロセッサを、こうしたMT1020Aチップ等のBluetooth制御部10に隣接して配備し、これを実行するという方式がある。

【0018】こうしたコンピュータプログラムでは、例えば、組み込み型の装置においてはLSIに内蔵されたARMプロセッサ上にあるプログラムとすることができ、又、パソコン等の情報処理端末に組み込む場合においては、当該情報処理端末のOS (Operating Systems: オペレーティングシステム) 上において作動するアプリケーションソフトウェアとすることができ、

【0019】図6は、Bluetoothの規格を説明するための図である。

【0020】この時、制御部20のプログラム(又アプリケーションソフトウェア)は、Bluetooth仕様で規定されている図6のソフトウェアレイヤの点線以上の部分を指す。特に、入力部12や表示部13の制御機能は、図6のApplicationに含まれる。

【0021】一方、点線以下の部分の機能は、上記のMT1020Aチップ等のBluetooth制御部10に実装されるのが一般的である。

【0022】無線送受信部11には、例えば、PHILSAR社 (<http://www.philsar.com>) のPH2401チップ等が用いられている。無線送受信部11は、Bluetooth制御部10とRadio-Interfaceを通して接続され、無線制御信号が送受される。

【0023】入力部12と表示部13については、例えば、Bluetooth機器に対して液晶ディスプレイやテンキー等を新たに組み込むことにより実現したり、又パソコン等に組み込む場合であれば、そのパソコンに備えられているディスプレイとキーボードを用いることができる。

【0024】

【発明が解決しようとする課題】上述したように従来の電子機器の認証システムでは、以下に述べるような問題点があった。

【0025】第1に、従来の電子機器の認証システムにおいては、認証相手の機器を識別するPIN-code等の識別情報を入力するために、テンキー操作部や液晶表示等の機能を備える必要があった。また、こうした液晶表示部やテンキー操作部等は、サイズも大きく高価な部品であるため、このように従来では、認証処理を実現するためには、機器に識別情報の入力機能を付加するための多くのコストを必要としていた。

【0026】第2に、従来のBluetooth機器等の認証システムを備える電子機器の多くでは、PIN-code等の相手機器を識別する情報を手作業により入力する必要があり、入力に手間が掛かりまた入力ミスが発生することが

あるという問題点があった。

【0027】本発明の第1の目的は、上記従来技術の欠点を解決し、簡便にPIN-code等の各機器の識別情報を相互に交換することのできる、電子機器の認証システムとその認証方法を提供することである。

【0028】本発明の第2の目的は、上記従来技術の欠点を解決し、電子機器における認証処理を、識別情報を交換する双方の機器の一つのスイッチの押下のみにより指示することのできる、電子機器の認証システムとその認証方法を提供することである。

【0029】

【課題を解決するための手段】上記目的を達成するため本発明の電子機器の認証システムは、自機を識別する識別情報のデータを記録する識別情報記憶部と、前記識別情報を接続相手の電子機器に対し発信する発信部と、前記接続相手の電子機器から発信される、前記接続相手の電子機器の識別情報のデータを受信する受信部を備え、利用者による認証を指示する操作に応じて、前記接続相手の電子機器との間で識別情報のデータを相互に交換し、受信した前記接続相手の電子機器の識別情報のデータに基づき認証処理を実行することを特徴とする。

【0030】請求項2の本発明の電子機器の認証システムは、前記識別情報を、ブルートゥース機器のPIN-codeとすることを特徴とする。

【0031】請求項3の本発明の電子機器の認証システムは、前記発信部及び前記受信部は、赤外線信号を用いて、前記識別情報のデータを送受することを特徴とする。

【0032】請求項4の本発明の電子機器の認証システムは、前記接続相手の電子機器との間における、識別情報のデータの相互の交換が無事に完了した場合にその旨を利用者に通知するための接続通知部を備えることを特徴とする。

【0033】請求項5の本発明の電子機器の認証システムは、前記接続通知部は、発光ダイオードの点灯により、識別情報のデータの相互の交換が無事に完了したことを利用者に通知することを特徴とする。

【0034】請求項6の本発明の電子機器の認証システムは、認証処理の実行に対しロックを掛けるロック機構を備え、前記ロック機構においてロックが掛けられている場合には、認証を実行しないことを特徴とする。

【0035】請求項7の本発明の電子機器は、自機を識別する識別情報のデータを記録する識別情報記憶部と、前記識別情報を接続相手の電子機器に対し発信する発信部と、前記接続相手の電子機器から発信される、前記接続相手の電子機器の識別情報のデータを受信する受信部を備え、利用者による認証を指示する操作に応じて、前記接続相手の電子機器との間で識別情報のデータを相互に交換し、受信した前記接続相手の電子機器の識別情報のデータに基づき認証処理を実行することを特徴とす

る。

【0036】請求項8の本発明の電子機器は、前記発信部及び前記受信部は、赤外線信号を用いて、前記識別情報のデータを送受することを特徴とする。

【0037】請求項9の本発明の電子機器は、前記接続相手の電子機器との間における、識別情報のデータの相互の交換が無事に完了した場合にその旨を利用者に通知するための接続通知部を備えることを特徴とする。

【0038】請求項10の本発明の電子機器は、前記接続通知部は、発光ダイオードの点灯により、識別情報のデータの相互の交換が無事に完了したことを利用者に通知することを特徴とする。

【0039】請求項11の本発明の電子機器は、利用者が認証の実行を指示するためのスイッチと、自機を識別する識別情報のデータを記録する識別情報記憶部と、前記識別情報を接続相手の電子機器に対し赤外線信号を用いて発信する発信部と、前記接続相手の電子機器から赤外線信号を用いて発信される、前記接続相手の電子機器の識別情報のデータを受信する受信部と、発光ダイオードの点灯により、識別情報のデータの相互の交換が無事に完了したことを利用者に通知する接続通知部を備え、前記スイッチによる認証の実行の指示に応じて、前記接続相手の電子機器との間で識別情報のデータを相互に交換し、受信した前記接続相手の電子機器の識別情報のデータに基づき認証処理を実行することを特徴とする。

【0040】請求項12の本発明の電子機器は、前記識別情報を、ブルートゥース機器のPIN-codeとすることを特徴とする。

【0041】請求項13の本発明の電子機器は、認証処理の実行に対しロックを掛けるロック機構を備え、前記ロック機構においてロックが掛けられている場合には、認証を実行しないことを特徴とする。

【0042】請求項14の本発明の電子機器は、前記ロック機構は、利用者が認証の実行を指示するためのスイッチを、鍵付きのシリンダー錠に連動させるものとすることを特徴とする。

【0043】請求項15の本発明の電子機器の認証方法は、利用者からの認証の実行の指示を受け付けるステップと、記録されている自機を識別する識別情報のデータを読み出し取得するステップと、前記自機の識別情報のデータを、接続相手の電子機器に対し発信するステップと、前記接続相手の電子機器から発信される、前記接続相手の電子機器の識別情報のデータを受信するステップを備え、利用者による認証を指示する操作に応じて、前記接続相手の電子機器との間で識別情報のデータを相互に交換し、受信した前記接続相手の電子機器の識別情報のデータに基づき認証を実行することを特徴とする。

【0044】請求項16の本発明の電子機器の認証方法は、前記識別情報を、ブルートゥース機器のPIN-codeとすることを特徴とする。

【0045】請求項17の本発明の電子機器の認証方法は、赤外線信号を用いて、前記識別情報のデータを送受することを特徴とする。

【0046】請求項18の本発明の電子機器の認証方法は、前記接続相手の電子機器との間における、識別情報のデータの相互の交換が無事に完了した場合に、その旨を発光ダイオードの点灯により利用者に通知するステップを備えることを特徴とする。

【0047】請求項19の本発明のコンピュータプログラムを記録した記録媒体は、コンピュータシステムを制御することにより電子機器の認証処理を制御する、コンピュータプログラムを記録した記録媒体において、利用者からの認証の実行の指示を受け付けるステップと、記録されている自機を識別する識別情報のデータを読み出し取得するステップと、前記自機の識別情報のデータを、接続相手の電子機器に対し発信するステップと、前記接続相手の電子機器から発信される、前記接続相手の電子機器の識別情報のデータを受信するステップを備え、利用者による認証を指示する操作に応じて、前記接続相手の電子機器との間で識別情報のデータを相互に交換し、受信した前記接続相手の電子機器の識別情報のデータに基づき認証処理を実行することを特徴とする。

【0048】請求項20の本発明のコンピュータプログラムを記録した記録媒体は、前記識別情報を、ブルートゥース機器のPIN-codeとすることを特徴とする。

【0049】請求項21の本発明のコンピュータプログラムを記録した記録媒体は、赤外線信号を用いて、前記識別情報のデータを送受することを特徴とする。

【0050】請求項22の本発明のコンピュータプログラムを記録した記録媒体は、前記接続相手の電子機器との間における、識別情報のデータの相互の交換が無事に完了した場合に、その旨を発光ダイオードの点灯により利用者に通知するステップを備えることを特徴とする。

【0051】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して詳細に説明する。

【0052】尚、以下本発明の各実施の形態においては、電子機器の相互間の認証処理を、Bluetooth（ブルートゥース）における最初の接続手続きであるペアリングを例に説明するが、これに限定されるものではなく、同様に他一般の電子機器間の認証処理に用いることができる。また、以下本発明の各実施の形態においては、2台の電子機器の相互間の認証を例に説明しているが、3台以上の複数の電子機器の相互の認証処理も、同様に行うことができる。

【0053】図1は、本発明の第1の実施の形態による認証システムを備えるBluetooth機器100の構成を示すブロック図であり、第1Bluetooth機器100と第2Bluetooth機器100との、相互にPIN-codeを交換する2台のBluetooth機器100を示している。

【0054】各Bluetooth機器100においては、図5の従来のBluetooth機器と同様に、Bluetoothによる通信を処理するBluetooth制御部10や、Bluetoothにおける無線通信を行う無線送受信部11を備えると共に、本実施の形態の認証処理を制御する制御部20、ペアリングの実行を指示するためのスイッチ21、各機器におけるPIN-code情報を記憶する識別情報記憶部22、各機器のPIN-code情報を接続相手の機器に対し通知する発信部23、接続相手の機器から発信される相手の機器のPIN-code情報を受信する受信部24、利用者に認証処理が無事に終了したことを通知するための接続通知部25を備えている。

【0055】制御部20は、Bluetooth機器100内に備えられる半導体メモリやその他の記録媒体に記録された認証処理を実行するコンピュータプログラムを、Bluetooth機器100内に備えられるCPUその他の半導体回路が読み出して、Bluetooth機器100内の各部の処理を制御することにより、以下に説明される本実施の形態の認証処理を実行する。

【0056】制御部20における認証処理を実行するコンピュータプログラムとしては、例えば、組み込み型ARMプロセッサ上で稼動するプログラム等を用いることができる。

【0057】スイッチ21は、機械的や電氣的やその他の方法により、利用者がON/OFFの操作を行うスイッチであり、利用者はスイッチ21を“ON”とすることにより認証処理の開始を指示する。

【0058】例えば、スイッチ21は、利用者により“ON”とされた場合には、制御部20に対してペアリング指示信号を発信する等の方法により、そのON/OFFを通知することができる。

【0059】識別情報記憶部22は、各機器に固有のPIN-codeを記憶するのであり、このため半導体ROMやその他の不揮発性メモリを使用することが好ましい。識別情報記憶部22に記憶されたPIN-code情報（つまり、PIN-codeのデータ）は、ペアリング時において読み出され、ペアリング相手の機器に送信される。

【0060】発信部23と受信部24は、赤外線やその他の手段により、ペアリング相手の機器との間で各機器のPIN-code情報を送受する。例えば、図1に示されるように赤外線信号をPIN-code情報の通信に用いる形態においては、発信部23と受信部24のそれぞれに赤外線発光部と赤外線受光部を用いればよい。

【0061】こうして発信部23は、識別情報記憶部22から読み出された自機のPIN-code情報を発信し、受信部24は、ペアリング相手の機器のPIN-code情報を受信して制御部20に送る。

【0062】接続通知部25は、LED（Light Emitting Diode：発光ダイオード）を備えて認証処理の完了時において発光させる等の方式により、利用者に対し認証

処理の成功を通知する。

【0063】また、Bluetooth制御部10や無線送受信部11においては、図5に示される従来のものと同様であり特別の処理を必要とするものではない。本実施の形態においては、双方のBluetooth機器の間でのPIN-codeの交換を簡易な操作により処理することによりペアリングの操作の手間を削減するため、PIN-codeの送受の機能に特徴を備えるのである。例えば、Bluetooth制御部10において処理される、相手機器のPIN-codeを受領した後の認証処理は、Bluetoothの仕様（「Bluetooth spec 1.0」）において規定されている通りを行う。

【0064】尚、図1においては、Bluetooth機器100内には本実施の形態の認証処理に必要とする部分のみをブロック図として表示しているが、各Bluetooth機器100は、別に各機器の固有の処理を実行するための装置を備えるものである。

【0065】図2は、本実施の形態の認証処理を説明するためのフローチャートである。

【0066】まず、PIN-codeを交換させたい、つまり初めてBluetooth通信接続させたい2台のBluetooth機器100を、そのペアリングのための通信を行う発信部23、受信部24を備える個所を向かい合わせて置く（ステップ201）。双方のBluetooth機器100は、赤外線等による、発信部23から受信部24への通信の方式やその信号の出力等に対応して、例えば数センチ位の距離等の、通信の可能な定められた距離に設置する。

【0067】このように本実施の形態では、ペアリング時においてケーブル等を必要としない。また、ここで双方のBluetooth機器100は、必ずしも机の上等に並べて設置することを必要とするものではなく、Bluetooth機器100を手持って発信部23や受信部24を備える個所を向かい合わせてもよい。

【0068】向かい合わせにした後に、双方のスイッチをONにする（ステップ202）。この時にONにする順序は問わないが、同時にONである状態が維持される必要がある。

【0069】スイッチがONになると、双方のBluetooth機器100は、各自の機器のPIN-code情報を発信部23より発信し、受信部24が相手の機器より発信されるPIN-code情報を受信し、これを制御部20に通知する（ステップ203）。

【0070】制御部20は、相手PIN-code情報を受け取るとこれをBluetooth制御部10に通知し、Bluetooth制御部10により、この相手PIN-code情報を元に通常のBluetooth接続手順に従って接続手続きを行う（ステップ204）。

【0071】接続手続きが完了すると、制御部20は、接続通知部25により利用者に対し接続手続きの完了を通知する（ステップ205）。

【0072】そして、利用者は、双方のBluetooth機器

100において接続手続きが完了したことを確認したら（ステップ206）、スイッチ21をOFFにしてペアリングを終了する。

【0073】以上の処理により、双方のBluetooth機器100のPIN-codeの相互交換が実行され、以後この双方のBluetooth機器100間において、通常のBluetoothによる通信を行うことができる。

【0074】また、ステップ203における、双方のBluetooth機器100間のペアリングの通信を、赤外線信号によりPIN-code情報を送受する場合を例に挙げると、次の用に処理が行われる。

【0075】まず、制御部20は、自機の識別情報記憶部22から自機のPIN-code情報を読み取り、これを赤外線信号上のビット列に変換しFEC（forward error correction）等の誤り符号を付加して、赤外線発光部である発信部23から繰り返し発光することにより、PIN-code情報をペアリング相手の機器に通知する。

【0076】そして、赤外線受光部である受信部24は、受光した赤外線信号をFEC等の誤り訂正処理を行った上で、相手機器のPIN-code情報を抽出することにより相手機器のPIN-code情報を取得することができる。

【0077】また、こうした赤外線信号への変換や、FEC等による誤り制御の処理は、制御部20ではなく、発信部23や受信部24の側において行うものとしてもよい。

【0078】また、接続通知部25による利用者への接続手続き完了の通知方法としては、例えば、接続手続き完了の旨を通知するためのLEDを備えてこれを点灯させる等の方法が可能である。この場合、点灯させたLEDは、ステップ206の接続手続きの完了確認後、スイッチ21が“OFF”にされた時等に消灯させる。

【0079】以上説明したように、本実施の形態による認証システムを備える電子機器であるBluetooth機器100では、従来においては面倒なPIN-code等の識別情報の入力操作を必要としていた認証の操作を、識別情報を交換する双方の機器において、一つのスイッチを押下するのみによる簡易な操作により指示することができる。

【0080】また本実施の形態においてBluetooth機器100は、図5の従来のBluetooth機器100におけるように、液晶ディスプレイ等の表示部13や、テンキー等の入力部12を備えるものであってもよい。これは、元々キーボードやテンキーが具備されている機器であるパソコンや携帯電話機等をBluetooth機器とする場合においても、本実施の形態の簡易な操作により実行される認証処理の機能を新たに備えることにより、相手機器の識別情報を手操作で入力する手間が解消されるのである。

【0081】また、個々のBluetooth機器100において各機器の固有の処理を実行するための装置を、本実施の形態の認証処理のために使用することも可能である。

例えば、パソコンや携帯電話機等の多くの機器においては、本実施の形態のスイッチ21の機能を実現することのできる入力ボタンや、接続通知部25の機能を実現することのできるLEDや液晶ディスプレイ等を備えており、こうした予め備える各部の機能を用いることにより、少ない機能を付加するのみにより本実施の形態のBluetooth機器100を実現することができる。

【0082】つまり、例えば、液晶ディスプレイ等の表示部13を備える機器においては、接続通知部25による接続手続完了の旨の通知をその液晶ディスプレイに対し行うことができる。また、赤外線信号の送受信機能についても、パソコンやノートパソコンやその他の携帯情報端末等の一部におけるように、これを予め備える機器も多く、こうした機器においては発信部23や受信部24を新たに備える必要はなく、その赤外線信号の送受信機能を用いて本実施の形態の識別情報の送受信を行うことができる。

【0083】次に、本発明の第2の実施の形態を説明する。

【0084】図3は、本発明の第2の実施の形態による認証システムを備えるBluetooth機器100aの構成を示すブロック図である。本実施の形態においては、第1の実施の形態の構成に加えて、Bluetooth機器100aの認証処理をロックするためのロック機構26を新たに備える。

【0085】ロック機構26は、ペアリングの実行の可否を指定するための鍵であり、正規の利用者の操作によるロックの設定や解除の操作を受け付ける。Bluetooth機器100aは、ロックが解除されている場合に限りペアリングを実行し、ロックを設定している場合にはペアリングを実行しない。

【0086】ロック機構26は、例えば、シリンダー錠や、回転ダイヤル式の鍵や、押しボタン式の鍵や、電子式の鍵や、その他のBluetooth機器100aにおいて備え付けることのできる鍵を用いることができる。

【0087】ロック機構26による、ペアリングをロックする方法としては、例えば、スイッチ21を鍵付きのシリンダー錠等に連動させる方式や、ロック機構26がロックされている場合には、ペアリングを指示するスイッチ21等の各部に電源を投入しない方式や、制御部20等がロック機構26の状態を検出し、もしロックされている場合においてはペアリングを実行しないものとする方式等が可能である。

【0088】以上説明したように、本実施の形態による認証システムを備えるBluetooth機器100では、ロック機構26を備えることにより、外部の者により不正に又は利用者の不注意等によって、Bluetooth機器100aのペアリングが実行されることを回避することができる。これにより、Bluetooth機器100aの不正使用等を防止することができる。

【0089】尚、上記各実施の形態の認証システムは、認証処理を制御する制御部20や、その他の機能をハードウェア的に実現することは勿論として、各機能を備えるコンピュータプログラムを、コンピュータ処理装置のメモリにロードされることで実現することができる。図4に示されるように、このコンピュータプログラムは、磁気ディスク、半導体メモリその他の記録媒体90に格納される。そして、その記録媒体からコンピュータ処理装置にロードされ、コンピュータ処理装置の動作を制御することにより、上述した各機能を実現する。

【0090】以上好ましい実施の形態及び実施例をあげて本発明を説明したが、本発明は必ずしも上記実施の形態及び実施例に限定されるものではなく、その技術的思想の範囲内において様々に変形して実施することができる。

【0091】

【発明の効果】以上説明したように本発明の電子機器の認証システムとその認証方法によれば、以下のような効果が達成される。

【0092】第1に、本発明の電子機器の認証システムでは、認証の操作を行うためのキーボードやディスプレイ画面等の大掛かりな装置を電子機器に備える必要がなく、赤外線等の送受信部やスイッチ等を備える簡易な構成により認証処理を実現することができる。

【0093】このため、ヘッドセットやLANアクセスポイント用ベースステーション等の、キーボードやテンキー等を具備していない機器においても、赤外線等の送受信部やスイッチ等による簡易な構成を付加するのみで、電子機器の相互間の認証処理を行うことができる。従来のように液晶表示部やテンキー操作部等を、各電子機器の識別情報の入力のためのために新たに備える必要がなくなる。

【0094】第2に、本発明の電子機器の認証システムでは、Bluetooth機器におけるペアリング等の認証のための操作を、双方の機器において一つのスイッチを押下するのみによる簡易な操作により指示することができる。

【0095】このため、元々キーボードやテンキーが具備されている機器であるパソコンや携帯電話機等を用いて、Bluetooth等の方式による認証を行う場合においても、相手機器の識別情報を手操作で入力する手間が解消されるため、各機器の接続操作が簡易な操作により実現される。

【0096】第3に、簡易な装置構成により、簡便に識別情報を相互に交換することができるため、認証処理を行うBluetooth等の電子機器の小型化と簡便な操作性が実現する。

【図面の簡単な説明】

【図1】 本発明の第1の実施の形態による認証システムを備えるBluetooth機器の構成を示すブロック図であ

る。

【図2】 本発明の第1の実施の形態の認証処理を説明するためのフローチャートである。

【図3】 本発明の第2の実施の形態による認証システムを備えるBluetooth機器の構成を示すブロック図である。

【図4】 本発明のその他の実施の形態による認証システムを備えるBluetooth機器の構成を示すブロック図である。

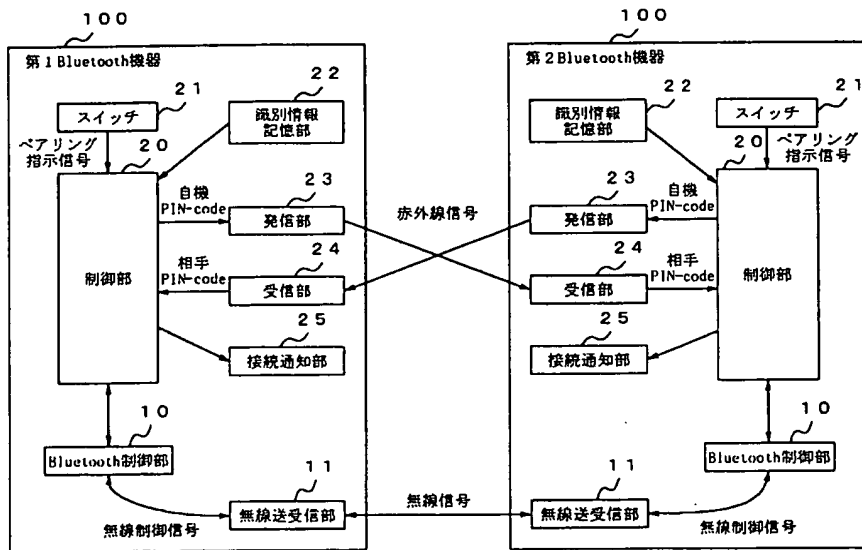
【図5】 従来のBluetooth機器の構成を示すブロック図である。

【図6】 Bluetoothの規格を説明するための図である。

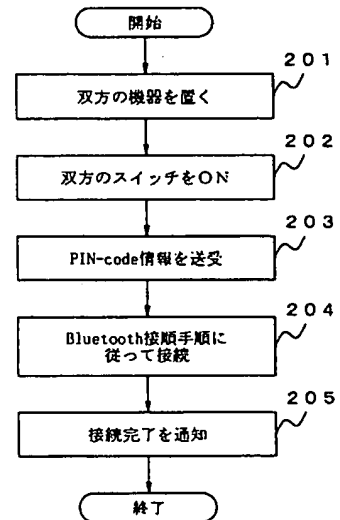
* 【符号の説明】

100、100a、100b、100c	Bluetooth機器
10	Bluetooth制御部
11	無線送受信部
20	制御部
21	スイッチ
22	識別情報記憶部
23	発信部
24	受信部
25	接続通知部
26	ロック機構
90	記録媒体

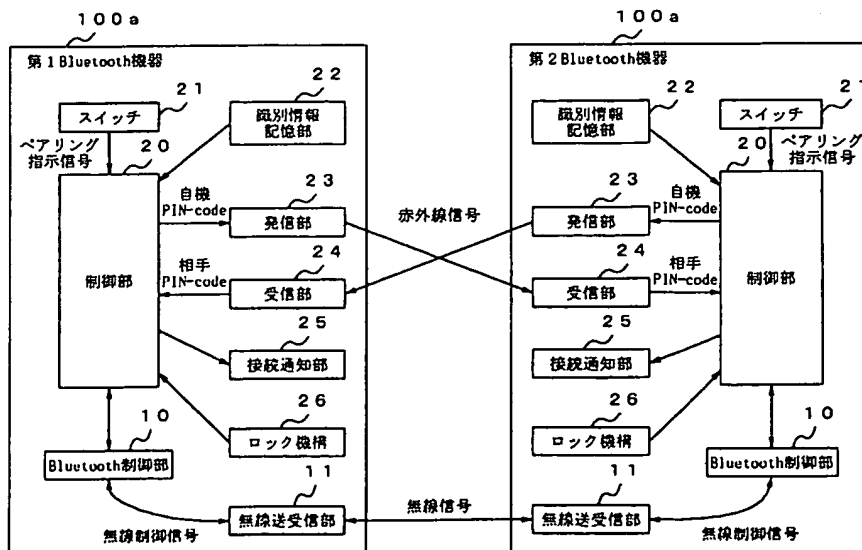
【図1】



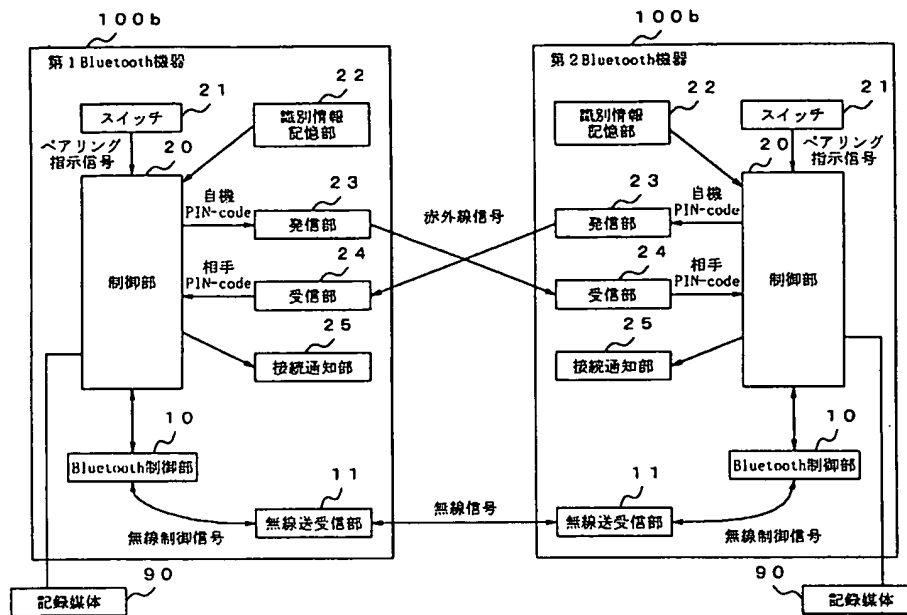
【図2】



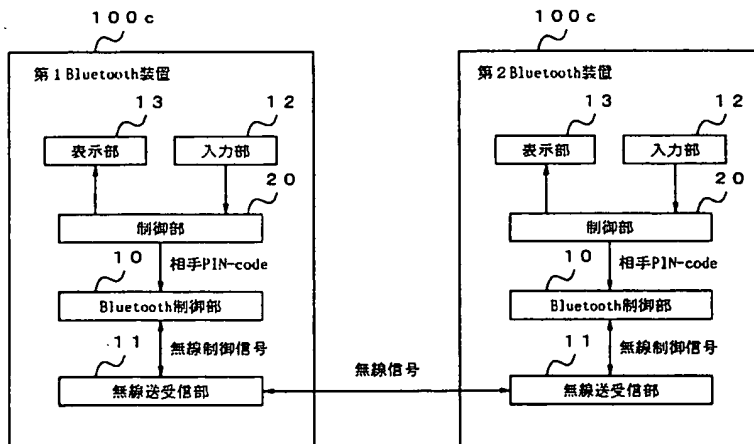
【図3】



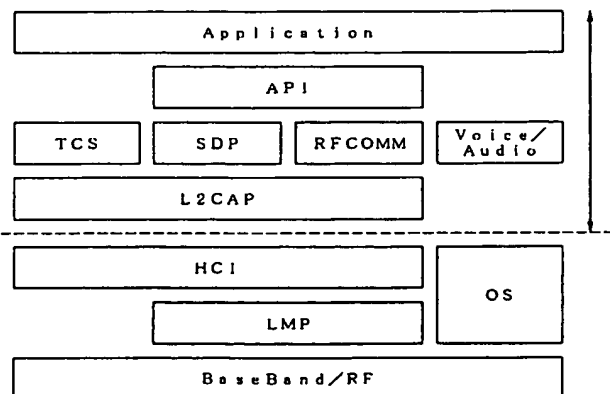
【図4】



【図5】



【図6】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.